Journal of the Association for Information Systems (2018) **19**(12), 1187-1216
**doi:** 10.17705/1jais.00524

RESEARCH PAPER

ISSN 1536-9323

# A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research

**Robert Willison[1], Paul Benjamin Lowry[2], Raymond Paternoster[3]**

[1]University of Jyväskylä, Finland., robert.r.willison@jyu.fi
[2]Virginia Tech, U.S.A., paul.lowry.phd@gmail.com
[3]University of Maryland, U.S.A., rpaterno@umd.edu

**Abstract**

This research-perspective article reviews and contributes to the literature that explains how to deter *internal computer abuse* (ICA), which is criminal computer behavior committed by organizational insiders. ICA accounts for a large portion of insider trading, fraud, embezzlement, the selling of trade secrets, customer privacy violations, and other criminal behaviors, all of which are highly damaging to organizations. Although ICA represents a momentous threat for organizations, and despite numerous calls to examine this behavior, the academic response has thus far been lukewarm. However, a few security researchers have examined ICA's influence in an organizational context and addressed potential means of deterring it. However, the results of these studies have been mixed, leading to a debate on the applicability of deterrence theory (DT) to ICA. We argue that more compelling opportunities will arise in DT research if security researchers more deeply study its assumptions and more carefully recontextualize it. The purpose of this article is to advance a deterrence research agenda that is grounded in the pivotal criminological deterrence literature. Drawing on the distinction between *absolute* and *restrictive* deterrence and aligning them with rational choice theory (RCT), this paper shows how deterrence can be used to mitigate the *participation in* and *frequency of* ICA. We thus propose that future research on the deterrent effects of ICA should be anchored in a more general RCT, rather than in examinations of deterrence as an isolated construct. We then explain how adopting RCT with DT opens up new avenues of research. Consequently, we propose three areas for future research, which cover not only the implications for the study of ICA deterrence, but also the potential motivations for these types of offenses and the skills required to undertake them.

**Keywords:** Computer Abuse, Internal Computer Abuse (ICA), Deterrence Theory (DT), Rational Choice Theory (RCT), Absolute Deterrence, Restrictive Deterrence, Security, Behavioral Security, Organizational Security, Information Security Policies (Isps), Compliance Violations, Criminal Behavior

Allen Lee was the accepting senior editor. This research article was submitted on August 26, 2016 and went through three revisions.

# 1 Introduction

Computer abuse (CA) is a pervasive phenomenon that is increasing globally in severity and importance. Broadly, CA can be said to involve a wide variety of criminally and noncriminally abusive behaviors inside and outside of formal organizations; however, this manuscript focuses on *internal CA* (ICA), which is criminal computer behavior committed by organizational insiders. The formal positions occupied by organizational insiders give them unique access to organizational information that is not afforded to outsiders. These insiders include current and former employees, consultants, managers and executives, members of boards of directors, and often industry partners and suppliers (Posey, Roberts, Lowry, Bennett, & Courtney, 2013, p. 168). ICA accounts for a large portion of insider trading, fraud, embezzlement, the selling of trade secrets, customer privacy violations, and other criminal behaviors, all of which are highly damaging to organizations.

Organizations are generally aware of and increasingly concerned about the magnitude of the threat posed by insiders.[1] Nonetheless, the academic response to the threat posed by ICA has been anemic, despite calls in a number of papers to focus on this research area.[2] For example, Mahmood et al. (2010) drew on the symbolic distinction found in "Wild West" movies between the black hat and the white hat: the "bad guys" wear the former, and the "good guys" wear the latter. Applying this distinction to information systems security (ISec) research, they noted an overemphasis on white-hat studies, especially in the area of employee compliance with organizational information security policies, and a corresponding scarcity of black-hat studies that focus on the behavior of those intent on engaging in some form of ICA. Mahmood et al. (2010) asserted the need to resist the temptation offered by white-hat research and to engage instead in harder-to-conduct black-hat studies. They argued that this shift could "elicit a virtuous cycle of research initiatives set in motion" (p. 432) and enable the development of improved safeguards based on the insights garnered from black-hat studies.

Despite the relative paucity of ICA research, one research area that has captured the attention of ISec researchers is deterrence. From a temporal perspective, the aim of deterring an individual from ICA precedes prevention efforts, which are designed to stop the actual commission process (Straub & Welke, 1998; Willison & Warkentin, 2013). That is, deterrence consists of using the threat of sanctions to inhibit conduct. The literature has generally assumed that the deterrence mechanism is perceptual, and the sanctions researchers have identified are both formal (e.g., censure by an organization) and informal (e.g., censure by a social group). ISec researchers have primarily applied deterrence theory (DT), originally developed in the field of criminology, to explain the dissuasion of insecure behaviors. The underlying assumption of perceptual DT is that would-be wrongdoers are sufficiently rational to be influenced by their knowledge of the consequences of criminal actions. Thus, DT asserts that if an individual perceives the chances of being caught committing a crime as high (i.e., *sanction certainty*), the associated penalties as severe (i.e., *sanction severity)*, and the penalties as meted out quickly (i.e., *sanction celerity*), then the individual will be deterred from carrying out a criminal act (Nagin, 1998; Paternoster, 2010). As such, DT is fully compatible with a rational choice model of behavior.

Deterrence efforts therefore provide an additional layer of IS security. Consequently, several studies have examined this phenomenon in an attempt to enhance its effectiveness in the organizational context. Unfortunately, the results of DT-based ISec studies have been mixed, leading to speculation regarding the merits of the theory (D'Arcy & Herath, 2011). We believe that one reason for these inconsistent results is that researchers often apply DT in *white-hat* studies of employee *compliance* with organizational information security policies or in *white-hat* studies of *noncriminal noncompliance* with such policies, but without the necessary step of strong theoretical recontextualization, which we explain below (see Appendix A).[3]

[1] For example, in 2014, Ernst & Young published its Global Information Security Survey, which consisted of 1,825 respondents from 60 countries (Ernst & Young, 2014). When asked about their most likely source of attack, the most common source was said to be employees (57%). The second most likely source consisted of contractors working on site (35%). Similarly, the 2015 PwC Global State of Information Security Survey reported that based on 9,700 respondents from 154 countries, current employees were the most cited cause of cybercrime (PwC, 2015). Notably, the second most cited cause was former employees (30%).

[2] There are several examples of such research calls (e.g., Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville, 2013; Lowry, Dinev, & Willison, 2017; Lowry, Posey, Bennett, & Roberts, 2015; Mahmood, Siponen, Straub, Rao, & Raghu, 2010; Posey et al., 2013; Willison & Warkentin, 2013).

[3] There are several examples of *white-hat* studies of employee *compliance* with organizational information security policies (e.g., Chen, Ramamurthy, & Wen, 2013; Herath & Rao, 2009a; Li, Zhang, & Sarathy, 2010; Pahnila, Siponen, & Mahmood, 2007a; 2007b; Siponen, Pahnila, & Mahmood, 2007; Siponen, Pahnila, & Mahmood, 2010;

Thus, these new contexts could actually generate creative, useful ideas. But the fundamental contextualization issue is that DT was designed not to motivate good behavior or to explain how to thwart noncriminal noncompliance, but to explain and predict how to thwart *criminal* or *antisocial* behavior. In the IS field, therefore, DT should translate into a focus on various forms of black-hat criminal behavior, including ICA. To use DT in such a radically different context, the theory needs to be carefully recontextualized and its new application justified. Simply applying a theory in a new context is not recontextualization (Boss, Galletta, Lowry, Moody, & Polak, 2015; Whetten, Felin, & King, 2009). Moreover, few IS studies have applied DT to ICA, and most of them are relatively old (e.g., Harrington, 1996; Hu, Xu, Dinev, & Ling, 2011; Lee & Lee, 2002; Lee, Lee, & Yoo, 2004; Peace, Galletta, & Thong, 2003; Straub, 1990; Straub & Welke, 1998; Willison, Warkentin, & Johnston, 2018).

Overall, it appears that the criminal roots of DT that are pertinent to ICA are largely overlooked in current ISec literature. This omission suggests that DT has been erroneously contextualized in most ISec studies because few of them have focused on criminal behavior, and the omission could be the reason for the disparate findings in the ISec DT literature. Unfortunately, there are mixed findings even among the studies that have applied DT to ICA, and as we argue later, this may be due to the manner in which DT has been conceptualized and applied as a stand-alone theory, despite its lack of resemblance to other social control theories (Paternoster, 1989b; Piliavin, Gartner, Thornton, & Matsueda, 1986). We posit that addressing DT in terms of both absolute and restrictive deterrence, and integrating these within the rational choice framework, represents a key omission in the ISec DT literature and therefore an important research opportunity that we address in this paper.

The remainder of this research-perspective article is organized as follows. In the next section, we review the DT-related research. We then describe the absolute and restrictive deterrence concepts and their application within the rational choice framework. Based on this foundation, we advance a revised agenda for deterrence-based studies of ICA, which consists of three areas for future research. We conclude by outlining the contributions of this study.

## 2 Literature Review: The Application of DT in ISEC Research

To establish the foundation for this study, we carefully reviewed the DT-related research that deals with ICA and information security policy (ISP) violations, while excluding non-DT-based studies. Unlike the review by D'Arcy and Herath (2011), ours involved only studies that addressed workplace computing and some aspect of DT; moreover, we reviewed working papers, books, and conferences in addition to journal articles. DT articles that focused on consumer-based computer crimes, such as digital piracy outside of the workplace by consumers or students (Gopal & Sanders, 1997; Higgins, Wilson, & Fell, 2005; Zhang, Smith, & McDowell, 2009), nonsecure behavior by consumers (James, Nottingham, & Kim, 2013), and hacking by outsiders (Young, Zhang, & Prybutok, 2007), were not reviewed. Moreover, DT-based studies on computer crimes committed by students (e.g., Dugo, 2007; Hollinger, 1993) were not included, and work for which the data were unavailable was not processed (Warkentin, Malimage, et al., 2012). Studies that were related to DT but did not directly use it or its related surrogate measures were also excluded (e.g., Choi, Levy, & Hovav, 2013). Finally, one study was omitted because all the deterrence effects it examined were at the organizational level (Schuessler, 2009). Appendix A provides a detailed summary of the articles that fell within the scope of our review.

In the literature review, several notable patterns emerged. First, virtually all studies used either cross-sectional surveys or factorial surveys based on hypothetical scenarios. The one exception, a study by Workman and Gathegi (2007), was a field experiment involving a control and two treatments as well as a follow-up measurement after six months to determine whether punishment and ethics interventions could decrease security policy contravention.

Second, most of the studies did not involve *actual* ICA behaviors that were malicious and criminal. Most involved ISP noncompliance/compliance *intentions* via self-report or through hypothetical scenarios. Other studies included malicious and nonmalicious compliance behaviors (e.g., D'Arcy & Hovav, 2009; Lowry et al., 2015). Only a few DT-based security studies actually provided empirical evidence of malicious, criminal ICA in the workplace (Harrington, 1996; Hu et al., 2011; Lee et al., 2004; Lowry, Posey, Roberts, & Bennett, 2014; Peace et al.,

Son, 2011). Likewise, several *white-hat* studies have examined *noncriminal noncompliance* with organizational security policies (e.g., Barlow, Warkentin, Ormond, & Dennis, 2013; Cheng, Li, Li, Holm, & Zhai, 2013; Guo & Yuan, 2012; Guo, Yuan, Archer, & Connelly, 2011; Siponen & Vance, 2010; Ugrin, Pearson, & Odom, 2008; Ugrin & Pearson, 2013; Warkentin, McBride, Carter, & Johnston, 2012; Workman & Gathegi, 2007). See Appendix A.

2003; Posey, Bennett, Roberts, & Lowry, 2011; Straub, 1990; Willison et al., 2018).

Third, as also noted by D'Arcy and Herath (2011), we found that the studies' operationalization of DT-sanctions constructs exhibited several pivotal disparities. Some adhered to DT by considering both the severity and certainty of sanctions (e.g., Cheng et al., 2013; Herath & Rao, 2009a; Herath & Rao, 2009b); however, only three studies also considered celerity—an integral part of DT—as a separate construct (Chuma, 2012; Hu et al., 2011; Lowry et al., 2015). Other studies, though they recognized severity and certainty (and sometimes celerity), combined all of these into one operationalized sanctions/deterrence construct rather than analyzing them individually (Barlow et al., 2013; Bulgurcu, Cavusoglu, & Benbasat, 2010; D'Arcy & Devaraj, 2012; Guo & Yuan, 2012; Guo et al., 2011; Siponen et al., 2007; Siponen et al., 2010; Siponen & Vance, 2010). Another large group of studies did not measure the DT constructs but instead used other constructs; such as security, education, training, and awareness (SETA) programs, security awareness, and ISPs, as general surrogates for sanctions (D'Arcy & Hovav, 2007; 2009; Fan & Zhang, 2011; Harrington, 1996; Lee et al., 2004; Straub & Welke, 1998; Ugrin et al., 2008; Ugrin & Pearson, 2013; Workman & Gathegi, 2007). Finally, one study showed no relationship between sanctions and intentions but did show relationships with formal risks, which in turn influence sanctions (Hu et al., 2011).

Fourth, most of the studies explored constructs that could plausibly be considered extensions of DT, such as informal sanctions, as well as several constructs that are unrelated to DT. Various forms of morality/moral and commitment/shame sanctions were used, which were sometimes justified as *informal sanctions* (e.g., Siponen & Vance, 2010). In other studies, informal sanctions were added from various morality theories (e.g., Hu et al., 2011). Other forms of informal sanctions included various types of social norms and pressures (Cheng et al., 2013). Because some studies examined compliance instead of noncompliance, several studies added the concept of rewards for good behavior (Chen et al., 2013; Pahnila et al., 2007a; Siponen et al., 2010).

Finally, although the purpose of DT is to explain how to deter criminal/malicious behaviors, several studies adopted the opposite approach and used DT to predict good behaviors. Most of these studies predicted ISP compliance intentions (Bulgurcu et al., 2010; Chen et al., 2013; Herath & Rao, 2009a; Herath & Rao, 2009b; Pahnila et al., 2007a; 2007b; Siponen et al., 2007; Siponen et al., 2010; Son, 2011). One study predicted IT security effectiveness (Kankanhalli, Teo, Tan, & Wei, 2003), another predicted Internet use policy compliance intentions (Li et al., 2010), and one predicted the intention to avoid Internet misuse (Liao, Luo, Gurung, & Li, 2009).

Unfortunately, even within the few studies that applied DT to ICA, there were mixed findings across their varied contexts, and these studies are quite dated (Harrington, 1996; Hu et al., 2011; Lee & Lee, 2002; Lee et al., 2004; Peace et al., 2003; Straub, 1990; Straub, 1986).

In light of these issues, we conclude that the conversation on DT's applicability and recontextualization to ISec should be in its beginning, rather than its end, stages. Although we certainly cannot rule out the possibility that the inconsistent outcomes in this literature are artifacts of the varied methods and contexts, we believe much more has yet to be learned about applying and recontextualizing DT in security contexts. These kinds of adaptations are not necessarily wrong or misguided; indeed, they could represent compelling new directions for DT research. However, such dramatic departures from DT would benefit from stronger recontextualizations of the theory and justifications of the theoretical changes. Consequently, DT could be built on more effectively—for example, by following the advice of Whetten et al. (2009) and Boss et al. (2015) on this contextualization process. [4] When theories are recontextualized, a thoughtful recognition of their assumptions and boundary conditions can bring to light many unexpected opportunities that enrich both the theory and our empirical work. We expand on this argument in the next section, where we introduce absolute and restrictive deterrence.

## 3 Defining Absolute and Restrictive Deterrence

As noted, a major drawback of ISec researchers' use of DT is the inconsistency of the research findings. Again, these could simply be artifacts of empirical research. However, we posit that several of the issues also begin at the conceptual level, which is the focus of the remainder of this paper. In a review of the ISec DT literature, D'Arcy and Herath (2011) discussed the failings of this body of research and proposed a series of recommendations for future studies. For instance, they argued that DT studies should do the following:

[4] An especially detailed and painstaking example of how such a theoretical recontextualization should occur in a security/privacy context was recently demonstrated in Wall, Lowry, & Barlow (2016). To date, this simply has not been done in recontextualizing DT to noncriminal ISP policy compliance, and it thus represents a strong theoretical opportunity that could dramatically improve the associated empirical research.

> *Incorporate the more comprehensive rational choice framework that accounts for both positive and negative consequences of behavior, especially since research indicates that perceived benefits have a strong influence on corporate offending decisions (Simpson et al. 2002). Assessing the impact of sanctions along with the competing influences of positive incentives provides a more complete understanding of the deterrence process* (pp. 655–656).

The authors noted that with the exception of one paper, the research articles focused solely on the traditional costs of formal sanctions. Notably, similar observations, dating back to the 1980s, had already been made in the field of criminology. Piliavin et al. (1986) argued that DT researchers had been preoccupied with the isolated effects of the severity and certainty of sanctions on illegal behaviors. They further asserted that it would prove more beneficial if DT were studied within an explicit theoretical framework, and to this end, they incorporated formal sanctions within a rational choice model. Aside from the consideration of these sanctions, the application of this type of model also allowed Piliavin et al. (1986) to examine the role of benefits/rewards in the criminal decision-making process. Thus, their model viewed the offender as calculating not only the expected utility/disutility of illegal actions but also the legal alternatives. They concluded that if the expected utility of illegal actions is perceived as greater than that of the legal alternatives, illegal actions will be more likely to occur.

Similarly, Paternoster (1989a; 1989b; 2010) observed that criminological DT research remained isolated from general theories of control and lamented the lack of theoretical and conceptual development since the seminal work of Gibbs (1975) was published. Acknowledging the advances made by Piliavin et al. (1986), Paternoster (1989a) aimed to extend this work by considering how DT could be more fully integrated into a rational choice framework. Paternoster argued that DT criminologists had failed to clearly delineate *which* criminal decisions would be influenced by formal sanctions. Thus, he stated that

> *neither classic nor more contemporary deterrence theorists have carefully specified the specific offending decisions that are to be affected by subjective assessment of the certainty and severity of punishment. As a result, deterrence researchers have not recognized that persons make several kinds of offending decisions that may be differentially affected by a given set of explanatory factors* (Paternoster, 1989b, p. 9).

To illustrate this point, Paternoster (1989a; 1989b) cited the work of several bodies of criminological research in which, despite their differing foci, it was acknowledged that offenders make several choices in the criminal decision-making process (e.g., Blumstein, Cohen, Roth, & Visher, 1986; Clarke & Cornish, 1985). As an illustration, Paternoster (1989a) noted the work of Blumstein et al. (1986) and their research on criminal careers (see also Blumstein, Cohen, & Farrington, 1988). In this context, the word *career* is used solely to describe the sequence of offenses during a period in the offender's life; it does not necessarily indicate that any earnings gathered through crime will form the basis of the offender's livelihood. Thus, researchers in this field emphasized that for an offender, there is a *beginning* (i.e., participation), *continuation* (i.e., career length), and *cessation* (i.e., end of criminal career). Related to these decisions is the criminal's *frequency of offending*, which refers to the number of offenses committed by an active offender.

Given these stages in the offender's decision-making process, Paternoster (1989a) crucially noted that a deterrence effect could take two forms and advanced a comprehensive rational choice model of delinquent offending. This model considers deterrence in the traditional manner, noting that an offender could be deterred from committing further criminal acts, which impacts the *frequency* of offending; however, the model also affords a specific consideration that an individual may be deterred from ever *participating* in a crime, or to use the terminology from Blumstein et al. (1986), whether or not there is a "beginning" to a criminal career. To substantiate his position, Paternoster (1989a) drew on the work of Gibbs (1975), who distinguished between *absolute* and *restrictive* deterrence. Gibbs (1975) described *absolute deterrence* as occurring when "an individual has refrained throughout life from a particular type of criminal act because in whole or in part he or she has perceived some risk of someone suffering a punishment as a response to the crime" (p. 32).

Consequently, in the ISec context, researchers would use the term *absolute deterrence* to describe the deterrence of organizational insiders from *ever* committing ICA. For example, if the fear of being detected has inhibited an insider from even attempting to use his or her office computer to commit some type of cybercrime, the person has been *absolutely deterred*. *Restrictive deterrence*, in contrast, has been defined as

> *the curtailment of a certain type of criminal activity by an individual during some period because in whole or in part the curtailment is perceived by the individual as reducing the risk that someone will be punished as a response to the activity* (Gibbs, 1975, p. 33).

Thus, in the ISec context, restrictive deterrence would apply only to insiders who have committed a form of ICA at least once and who will have to decide whether or not to engage in another crime.

Clarke and Cornish (1985) advanced their rational choice theory (RCT) perspective four years earlier than Paternoster's (1989a) position on absolute and restrictive deterrence. They argued that criminals make what are termed *involvement* and *event* decisions. Regarding the involvement decisions, they noted like Paternoster that an offender makes a series of choices related to the three stages of a criminal career (Blumstein et al., 1986), that is, in terms of "beginning" criminal activity (i.e., *initial involvement*; described by Paternoster as *participation*), whether to continue (continuation), and when to stop (cessation). Event decisions are choices made during the perpetration of a crime. Clarke and Cornish's work on RCT has evolved into a seminal criminological model (cf. Cornish & Clarke, 2014).

To highlight the differences between the decision stages, Clarke and Cornish (1985) depicted the stages in a series of models, using burglary in a middle-class suburb as an example. These models served as schematic representations, illustrating the key decision points in criminal behaviors. Accordingly, of specific relevance to the application of absolute deterrence is their *initial involvement* model, which is similar to Paternoster's (1989a) discussion of *participation*, as noted. More specifically, Clarke and Cornish's initial involvement model allowed for the consideration of the benefits and costs associated with the legitimate/illegitimate alternatives as well as the potential costs incurred through the *likelihood* and *severity of punishment*—the two constructs central to DT. Thus, as in Paternoster's research, Clarke and Cornish recognized the possible influence of (absolute) deterrence at the *initial involvement/participation stage*.

## 4 A Revised Deterrence Research Agenda for Security Research

As our literature review shows, although ICA represents a major threat for organizations, and despite numerous calls to examine this form of behavior, the academic response has been underwhelming. Of course, this means the conversation on DT's application to ICA has many remaining opportunities. Although some studies have used DT to improve the understanding of ICA, the manner in which some studies have done so can be characterized as not fully realizing the possibilities and assumptions of DT—and this has led to mixed outcomes. For instance, the literature review suggests that ISec research should refocus on black-hat behavior rather than just examining nonmalicious behavior; furthermore, ISec researchers would benefit from basing their work on actual security behaviors instead of hypothetical behaviors. However, these well-known and straightforward points are not the focus of this article. Instead, the major contribution of this study is to challenge and extend, on the basis of criminological research, the actual conceptualization of deterrence itself. After examining the key criminological studies of Paternoster (1989a) and Clarke and Cornish (1985), we argue that ISec research should undertake a fundamental shift: it should rethink the conceptualization of deterrence itself in order to account for rational forces and absolute and restrictive deterrence.

Before we discuss three related areas for future research, we argue that DT should be extended using an RCT perspective. Paternoster (1989a) and Piliavin et al. (1986) were keen to address a limitation of previous criminological deterrence studies, which had been preoccupied with studying the isolated effects of the severity and certainty of sanctions on potential illegal behaviors. They argued that on their own, these formal sanctions bore little resemblance to more general theories of social control. To address this limitation, Paternoster (1989a) incorporated formal sanctions within an RCT model of offending, which offered a "fully specific model of social control" (p. 289). Table 1 lists the key explanatory factors included in Paternoster's DT/RCT choice model of participation and frequency of involvement in four minor delinquent offenses.[5]

Deterrence researchers from the field of criminology are not the only researchers who have been "preoccupied" with formal sanctions. This is also the case for ISec researchers. As D'Arcy and Herath (2011) noted in their review of the deterrence literature, with the exception of one paper, the assessed research articles focused solely on the traditional costs of formal sanctions.

[5] Although Paternoster (1989a) proposed the application of RCT, he did not examine the potential benefits that could be accrued through either legitimate or illegitimate actions.

**Table 1. Key Explanatory Factors of Paternoster's (1989a) DT/RCT Model**

| Explanatory factor categories | Example factors |
|---|---|
| Demographic background factors | • Gender<br>• Family structure<br>• Assistance |
| Delinquent opportunities | • Parental supervision<br>• Social activities with peers<br>• Peer involvement in delinquency |
| Nondelinquent lines of action | • Desired education<br>• Expected education<br>• Expected occupation<br>• Grades<br>• Commitment to school<br>• Religious activities<br>• General conventional commitments |
| Valued social relationships | • Attachment to father<br>• Attachment to mother<br>• Attachment to teachers<br>• Attachment to best friends |
| Informal sanctions for delinquency | • General informal sanctions<br>• Peer sanctions for specific delinquent act<br>• Parental sanctions for specific delinquent act |
| Formal legal sanctions | • Perceived certainty of punishment<br>• Perceived severity of punishment<br>• Caught by the police for prior delinquency |
| Moral commitments | • Moral beliefs against specific delinquent acts |
| *Note:* Table adapted from Paternoster (1989a, p. 294). | |

One reason for the mixed findings in ISec deterrence research may simply be that on their own, formal sanctions do not reflect any theory of social control. We believe the RCT framework provides a more comprehensive and accurate reflection of the factors an individual will consider as part of the decision to become involved in crime at the "initial involvement" stage. [6] These factors include deterrence sanctions. Thus, the offender is viewed as calculating not only the utility/disutility of illegal actions, but also that of legal actions. It can therefore be predicted that if the expected utility of illegal actions exceeds that of the legal alternatives, an individual will be more likely to decide to engage in a specific crime at a later date (i.e., they will have reached a state of "readiness"). Moreover, we propose the use of the RCT framework for the future development of ICA research, because it has proven its value in studies of general criminal conduct (Matsueda, Kreager, & Huizinga, 2006; Piliavin et al., 1986).

Without a recognition of the range of factors incorporated within RCT and their relationship with DT constructs, we could find ourselves stuck with overly simplistic models that do not reflect reality. Implementing these factors would answer the call for more comprehensive accounts of how deterrence can occur and would avoid an oversimplified understanding of offender behaviors based on the certainty and severity of punishment (Piliavin et al., 1986). This is particularly compelling, because substantial expertise on both perspectives exists in our research community; we just have to combine these forms of expertise to realize their potential.

We now move on to a discussion of three areas for future ISec DT research.

## 4.1 Research Area 1: Absolute Versus Restrictive Deterrence

Advancing the application of an RCT model enables the consideration of the relationship between deterrence and the different stages in the criminal decision-making process. It is important for security researchers to recognize that offenders engage in a

[6] Importantly, this is a key departure from Bulgurcu et al. (2010), who partially used RCT to predict *compliance intentions*, and Hu et al. (2011), who mixed DT, RCT, and a couple of other theories in predicting noncompliance intentions. Both overlook initial involvement and actual behaviors.

number of choices during the criminal decision-making process (Blumstein et al., 1988; Blumstein et al., 1986; Clarke & Cornish, 1985; Hagan, 1997; Piquero & Benson, 2004; Sampson & Laub, 1995). Indeed, this view is now so firmly entrenched within the criminological discipline that a subdiscipline called *developmental criminology* has emerged (Farrinton, 2003; Piquero, 2008; Sampson & Laub, 2005). This strand of research has also confirmed that in addition to making decisions regarding the crime event (which impact the frequency of crime), offenders make choices regarding their *participation* in, *continuation* of, and *desistance* from crime.

On the basis of these insights, we assert that RCT is a highly promising framework for conceptualizing and studying absolute deterrence. Indeed, when considering sanctions as potentially influencing factors, the articulation of these decisions allows for the application of deterrence for two different aims. As noted, one aim is that sanctions effectively deter individuals from ever participating in crime (i.e., absolute deterrence). The second aim is to reduce the frequency of offending (i.e., restrictive deterrence*)*.

Drawing on RCT and applying the absolute deterrence concept can thus provide a far better understanding of where the influence of deterrence occurs in the criminal decision-making process. More specifically, (absolute) deterrence can initially exert an influence in the *participation* stage as opposed to the *event* stage. In terms of existing ISec DT studies, deterrence will first exert an influence not in the formation of intention but rather prior to it. This understanding is enhanced when absolute deterrence at the participation stage is considered, as illustrated by the work of Clarke and Cornish (1985), which is depicted in Figure 1.

Unlike Paternoster (1989a), who conducted his research through surveys, Clarke and Cornish (1985) drew on offenders' accounts of burglary in the development of their decision-making models. As highlighted, of specific relevance to the current discussion is their *initial involvement* model (see Figure 1), which reflects the stage Paternoster referred to as *participation*. In essence, the model is a graphical depiction of RCT. Thus, the Clarke and Cornish model offers significant clarity regarding the factors of influence in this stage of the criminal decision-making process, and we therefore advocate its use in conceptualizing absolute deterrence at the *initial involvement/participation* stage.

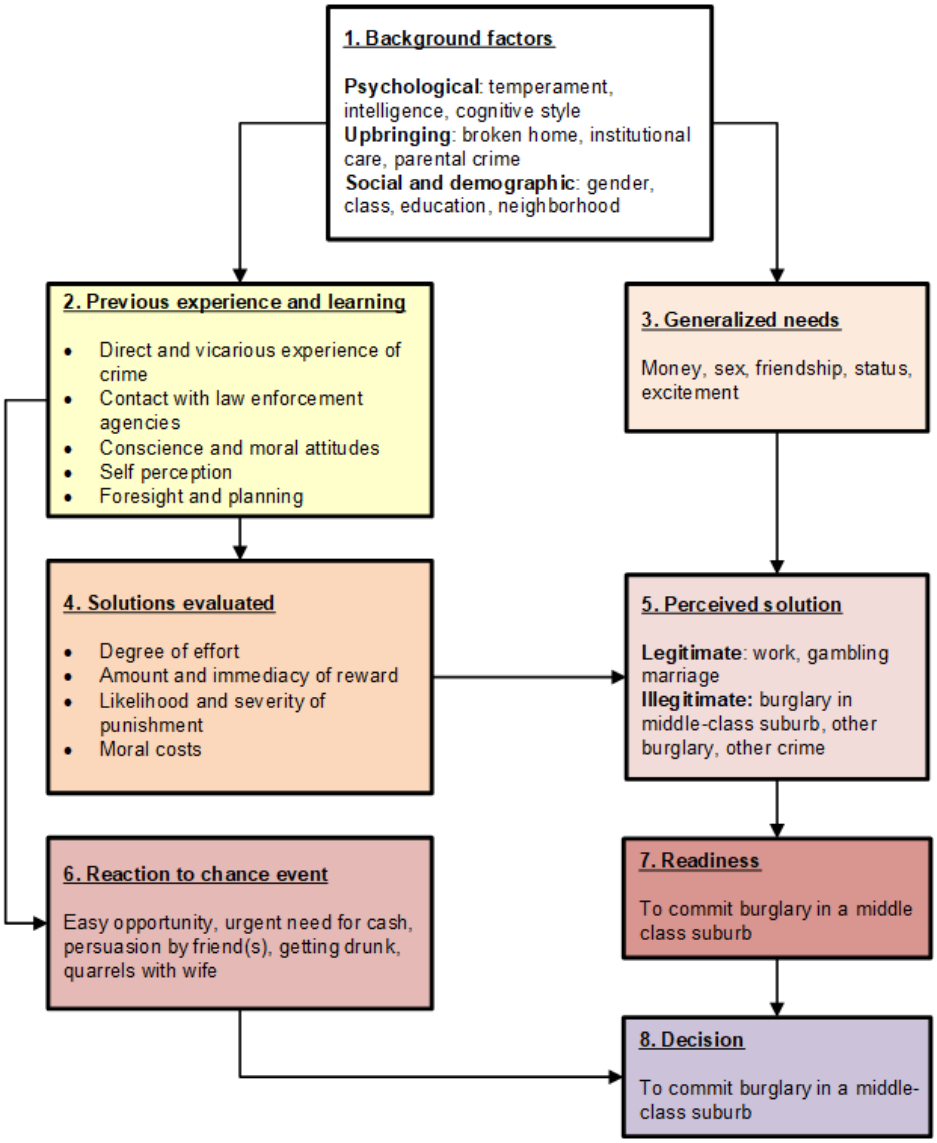


**Figure 1. Clarke and Cornish (1985) Initial Involvement Model**

There are two key decision points in this model. The first is when an individual has reached a state of *readiness* (Box 7). As Clarke and Cornish (1985, p. 167) noted,

> *Readiness involves rather more than receptiveness: it implies that the individual has actually contemplated this form of crime as a solution to his needs and has decided that under the right circumstances he would commit the offence.*

Thus, in reaching a state of *readiness*, individuals will not be considering the perpetration of a specific offense but whether an offense will act as a solution to their needs (Box 3). This state will have been informed by a consideration of possible solutions (Box 4) to these needs and whether they can best be met through legitimate or illegitimate means (Box 5).

Accordingly, not only does such a model allow for the consideration of the benefits and costs associated with the legitimate/illegitimate alternatives, but it also includes the potential costs that could be incurred through "the likelihood and severity of punishment" (Box 4), that is, the two central constructs of DT. The appraisals made in Box 4 will also be influenced by an individual's self-perception, moral code, and previous experience with crime and the extent to which planning/employing foresight is possible (Box 2). In addition, Boxes 2 and 3 will be influenced by what Clarke and Cornish (1985) termed *background factors* (Box 1). These factors are examined using criminological theories that explain how individuals develop criminal dispositions. Typically, these theories examine psychological, familial, and sociodemographic factors.

The second key decision in the initial involvement model is Box 8, which refers to the decision to

commit a burglary. It is important to note that Clarke and Cornish (1985) modeled this decision separately and referred to it as their *event* model. Therefore, (absolute) deterrence initially exerts an influence at the *participation* stage, when an individual is evaluating potential solutions (Box 4) and how this further influences potential "perceived solutions" (Box 5). If the perceived solution is deemed to be criminal in nature, then the individual has reached the state of *readiness*, and at a later point in time, the criminal event may or may not occur.

Given the above discussion, we now advance our first question for future research:

**Future Research Question 1:** Which factors exert an absolute deterrence influence at the initial involvement stage of the criminal decision-making process?

As noted, in the RCT framework, formal deterrence sanctions form only part of the influences at the initial involvement stage. This then raises the question of what other types of deterrence factors will be influential at the initial involvement stage, particularly in view of the focus on ICA and the people who could possibly perpetrate this form of crime. Although Clarke and Cornish (1985) cited only formal sanctions, there is no reason the range of sanctions based on Paternoster's (1989a) study could not be considered for the *initial involvement model*. Table 2 therefore represents our attempt to revise the factors from Paternoster's study for the organizational context with regard to ICA. This is in keeping with the work of Clarke and Cornish, who acknowledged that the configuration of the models will differ according to the type of crime under consideration. However, we urge careful contextualization as ISec researchers consider these factors.[7] Given our focus on ICA, examining the concept of shame may prove fruitful. Several criminological rational choice studies have used this self-imposed sanction to understand its influence on the deterrence process (Grasmick, Bursik, & Kinsey, 1991; Grasmick & Green, 1980; Nagin & Paternoster, 1993; Paternoster & Simpson, 1996; Piquero & Tibbetts, 1996). The need to develop an understanding of these informal sanctions would thus be of paramount importance, because these studies have emphasized that employees are particularly vulnerable to this form of cost given their stake in conventional society (Willison & Warkentin, 2013). In addition, mainstream criminological DT research has noted that there is now greater confidence that nonlegal factors, as opposed to formal sanctions, can ensure deterrence (Paternoster, 2010).

We conclude this section by noting that this research area, and the other two we are about to propose, provide excellent opportunities for ISec researchers to move from the limited idea of the IT artifact to the more general idea of the IS artifact, as proposed by Lee, Thomas, & Baskerville (2015). We share the view of Lee et al. and of Currie (2009), who maintained that there needs to be a better distinction between the IT artifact and its context, which could include the organizational, social, and environmental factors of a system's implementation.

[7] A key process in theory building from one discipline to a new discipline is to carefully rethink and recontextualize factors from a source context to a new context and to carefully challenge and examine the underlying theoretical assumptions, because not everything may hold in the new context or in the same way (Boss et al., 2015; Whetten et al., 2009). Thus, great care should be taken to recontextualize the factors from criminology into appropriate ISec factors.

**Table 2. DT/RCT Model Factors Adapted to Thwarting ICA in an Organizational Context**

| Explanatory factor categories | Example factors |
|---|---|
| Demographic background factors | • Gender<br>• Family responsibilities<br>• Job type<br>• Education level<br>• Salary |
| ICA opportunities | • Direct supervision from management<br>• Social activities with coworkers<br>• Coworker involvement in ICA<br>• Access to confidential data and open-access systems<br>• System monitoring and logging |

**Table 2. DT/RCT Model Factors Adapted to Thwarting ICA in an Organizational Context**

| | |
|---|---|
| Noncriminal lines of action | • Desired promotion<br>• Professional viewpoint toward occupation<br>• Annual performance review<br>• Commitment to organization<br>• Religious activities<br>• General conventional commitments |
| Valued social relationships | • Attachment to family<br>• Attachment to coworkers<br>• Attachment to supervisor<br>• Attachment to best friends |
| Informal sanctions for delinquency | • General informal sanctions<br>• Peer sanctions for specific ICA act<br>• Supervisor sanctions for specific ICA act |
| Formal legal and organizational sanctions | • Perceived certainty of punishment<br>• Perceived severity of punishment<br>• Caught by the police for prior ICA<br>• Caught by organization for prior ICA<br>• Knowledge of law<br>• Knowledge of applicable organizational policies |
| Moral commitments | • Moral beliefs against specific ICA acts<br>• Organizational membership or licensing requirements against ICA (e.g., certified CPA)<br>• Tendency to employ neutralization |
| *Note:* Table adapted from Paternoster (1989a, p. 294) to the ICA context. | |

From an organizational security perspective, this strongly resonates with us. Thus, we encourage ISec researchers to identify the "security artifacts" that matter and to address the proposed research questions accordingly. Ideas for related future research could easily fill another paper, so we will present only a couple of in-depth examples: for initial deterrence, it is important to consider factors other than formal and informal sanctions, and instead to think about which kind of IS artifacts could deliver or influence such sanctions, such as system design for enhancing social visibility or monitoring, system alerts, organizational interventions such as co-located working and job sharing, training interventions, and so on.

## 4.2 Research Area 2: Motivations for ICA at Initial Involvement

The next area we propose for future deterrence research relates to a consideration of the motivations for ICA. When Clarke and Cornish's (1985) *initial involvement* model was discussed, it was noted that it is useful for highlighting when deterrence influences occur in the criminal decision-making process; however, the model also assists in clarifying the relationship between the factors of influence at the *participation* stage, including factors that may motivate individuals to consider participating in ICA. Given the focus on intention in the ISec deterrence literature, the issue of *participation* has been overlooked along with the motivational factors that occur at this stage. For example, despite citing Cornish and Clarke (1986), who discussed the initial involvement model, Hu et al. (2011, p. 58) argued,

> *We submit that when an individual is presented with an opportunity to commit policy violations, his or her behavior depends on the rational calculus of the costs and the benefits.*

Therefore, to advance a clearer understanding of these motives, the *initial involvement* model is again advocated. As highlighted, Clarke and Cornish (1985) acknowledged that numerous criminological theories have been proposed for explaining how individuals come to develop criminal dispositions, which cause individuals to be more inclined to acts of a criminal nature. These theories (Agnew, 1992; Cloward & Ohlin, 2013; Hirschi, 2002) have noted the role of influences, which may include specific social factors (e.g., poor housing, low-quality education), psychological influences (e.g., mental illness), or the inheritance of traits (e.g., low self-control). Clarke and Cornish recognized the role of these influences in their *initial involvement* model and described them as background factors (see Box 1). In addition, they argued that the influence of such factors on an individual's decision to *participate* in crime would be moderated by "situational" and "transitory" forces. Indeed, advancing the example of computer fraud as a

case in point, they further asserted that for certain types of crime, background factors, and therefore the extent to which dispositional theories can help to explain *participation*, may be of far less relevance than an individual's immediate situation.

For ISec research, the influence of these situational and transitory forces is evident in a series of ongoing studies conducted by the U.S. Secret Service and the CERT Division based at Carnegie Mellon University. Their research has determined that a problem in an employee's personal life can influence his or her actions in the workplace. Thus, a report by Cappelli, Keeney, Kowalski, Moore, & Randazzo (2004) focused on the U.S. banking and finance sector. In the 23 cases of ICA examined, 27% of the perpetrators were experiencing financial difficulties in their private lives. These findings were echoed in a later CERT publication (Cappelli, Moore, & Trzeciak, 2012), which noted the interplay between the spheres of personal and work lives. When discussing incidents of computer fraud, they noted (p. 115),

> *The lives of insiders who committed fraud in our cases were often in turmoil . . . insiders often have severe financial problems. In addition, insiders had other personal issues such as a family member with health problems, substance abuse and physical threats by outsiders.*

Cappelli et al. (2012) subsequently noted the role of what they termed "stressors" in motivating computer fraud. More specifically, they categorized these stressors as *internal* and therefore as workplace occurrences (e.g., the threat of company layoffs, an employee not receiving an expected pay raise). Alternatively, stressors could be *external* to the workplace context—that is, occurring in employees' private lives (e.g., expensive hospital bills, gambling addiction).

Evidence for situational and transitory influences can also be found in the white-collar literature, which has examined this type of offense committed by individuals for their own gain, as opposed to employees who perpetrate white-collar crimes for the benefit of their companies (Weisburd, 1991; Weisburd & Waring, 2001; Wheeler, Weisburd, Waring, & Bode, 1988). As discussed, criminological dispositional theories and the various influences they advance in creating dispositions have been categorized by Clarke and Cornish (1985) as background factors (see Box 1). These theories, which have been developed to explain delinquency or street crimes, posit that for these groups of offenders, the *participation* in crime occurs early in life and during but not after adolescence (Blumstein et al., 1986; Piquero & Benson, 2004); however, this is contrary to white-collar offenses in which *participation* occurs much later in life, as evidenced in studies by Benson and Kerley (2000) and Weisburd and Waring (2001). They found that white-collar offenders were around the age of 40 when they chose to participate in crimes. To explain this finding, Piquero and Benson (2004) noted the role of situational influences, and they emphasized the presence of a crisis in either an individual's work or personal life as a critical factor. This mirrors previous white-collar research, which advocated focusing on contemporaneous problems experienced by individuals in either their work or personal lives to explain their participation in such offenses. As Benson and Kerley (2000, p. 133) noted,

> *One searches in vain for early precursors or early hints of trouble in the life-history of the typical white-collar offender. For most of these individuals, their offences appear to come out of nowhere. Their crimes do not appear to be part of longstanding patterns of anti-social conduct, nor do they appear to be deeply rooted in a troubled social background. . . . White-collar crime appears to be more a function of adult life experiences as opposed to latent personality traits or disturbed social background.*

Given the above discussion, we now advance our second research question:

**Future Research Question 2:** What are the situational and transitory factors that motivate ICA at the initial involvement stage?

It is important to note that these factors are not IS-specific. This is obviously the case for external factors, such as financial problems due to a divorce, medical bills, and various addictions; however, it is also the case for internal factors, such as when the threat of redundancy or the failure of being promoted may motivate individuals. These internal motivations are common to all employees.

It should also be noted that it is only by recognizing the different decision-making stages and the decisions and behaviors at each stage that a clear overview of the criminal process is afforded. Thus, we have demonstrated in this section that the initial involvement model allows for consideration of the motivational factors; however, the model also allows for consideration of the relationships between these motivational factors and the issues of deterrence. Clarke and Cornish (1985) suggested that these situational and transitory forces moderate background factors (again, Figure 1, Box 1), which influence "previous experience and learning" (Box 2) and "generalized needs" (Box 3). It is therefore likely that these situational and transitory forces influence the offender's "generalized needs." Future research could consider the extent to which the influence of

deterrents in the "solutions evaluated" stage (Box 4) is strong enough to lead to a perceived legitimate solution (Box 5).

As noted, the ISec deterrence literature has generally assumed that the motivations of an offender can be understood in terms of the factors that influence intention. Without an appropriate understanding of the *participation* stage, ISec researchers may continue to relate all motivating influences to intentions and thereby conflate causal relationships. We believe this research area, in addition to that of the IS artifact, is ripe for the use of real-time big-data analytics to create predictive models of potential readiness based on previous incidents. Such management "alerts" could direct management to people who are likely in need of more support and oversight, so that their readiness does not turn into action. Although there would be ethical concerns with such research and practice, organizations have already made legal use of predictive analytics to predict factors, such as which employees are most likely to quit prematurely, and to use this information to help them (Hewlett-Packard has done so to great effect). Organizations would not be privy to all key life events that could trigger ICA, but they are legally privy to some that could be studied in a consistent, predictive manner (e.g., change in marital status, surviving a round of layoffs in a department, credit score changes, change in number of family dependents, poor work reviews).

## 4.3 Research Area 3: Skills and Abilities of Offenders at Initial Involvement

Our third area for future research pertains to the skills and abilities of insiders who plan ICA, how these skills and abilities relate to the organizational context in which they work, and how this relationship can influence decision-making at the initial involvement stage.

As noted, Clarke and Cornish (1985) acknowledged that the configuration of the initial involvement model will differ according to the type of crime under consideration. Thus, as indicated in Box 2 of their initial involvement model, it is unlikely that insiders will have "direct and vicarious experience with crime" and "contact with law enforcement agencies"; however, employees certainly have the ideal location and the necessary time to undertake "foresight and planning," given that they work in the very environment in which the crime would occur. This is unlike the vast majority of other crimes; thus, differences such as these need to be acknowledged and considered in terms of their influence at the initial involvement stage.

The issue of how potential offenders plan for ICA has received little attention in the ISec field. The ISec studies in this area have focused mostly on the intention for this type of behavior, and the focus has therefore remained on the act of perpetration (i.e., D'Arcy & Devaraj, 2012; D'Arcy & Hovav, 2007; 2009; D'Arcy, Hovav, & Galletta, 2009; Harrington, 1996; Hovav & D'Arcy, 2012; Hu et al., 2011; Lee et al., 2004; Lowry et al., 2015; Peace et al., 2003).

Yet, it should be recognized that this focus is based on the assumption that any influences must relate to this construct. However, and as noted, the RCT framework provides a much clearer insight into offender decision-making and the associated influences at the initial involvement and event stages. Thus, at the initial involvement stage, consideration can be given to the planning process and its role in influencing an individual's participation decision.

Despite the paucity of research on the topic, some ISec studies have considered the offender-context dynamic and its implications for planning. To investigate what constitutes an opportunity for ICA, Willison (2006) drew on insights from environmental criminology (Brantingham & Brantingham, 1991) to highlight the role of *awareness spaces* for potential offenders. For street offenders, these spaces may encompass the neighborhoods in which they live. Through their daily activities, such as traveling to work and going shopping, offenders become aware of potential opportunities, such as a car to steal or a convenience store to rob. What distances employees from street offenders is that they spend a large part of their days in the very context in which offenses are subsequently committed. Therefore, unlike street offenders, dishonest employees have the luxury of spending a considerable amount of time recognizing potential opportunities. Such recognition may remain purely innocent, but a change in personal circumstance may force a reconsideration of whether to act on them.

The idea that potential offenders use information from their environment to search for and assess potential opportunities is also consistent with Clarke and Cornish (1985), who in their work on RCT argue that offenders are limited by "bounded rationality." That is, criminal decision-making is at times less than perfect, as a consequence of the conditions under which decisions are made. As a result of the risks and uncertainty associated with offending, criminals may make decisions without the knowledge of all the potential costs and benefits (i.e., the risks, efforts, and rewards). Lacking all the necessary information, criminals may resort to "rules of thumb" or heuristics when perpetrating offenses, or they may rely on a tried and tested general approach that may be called into action when unexpected situations arise. When this is considered in relation to the quality of information used to inform ICA decisions, it could be argued that some insiders have access to near-perfect information when planning potential offenses.

Although the organizational context can, in the above light, be seen to benefit offenders, the white-collar literature has also noted that the specific roles employees undertake in various departments can be a delimiting factor with regard to the types and forms of ICA abuse they can undertake. For example, Piquero and Benson (2004) noted that, unlike street offenders' opportunities, those of white-collar criminals are not ubiquitous or so democratically distributed. Rather, they argued that access to opportunities are shaped by the occupational position undertaken by employees and the abilities/skills required to discharge the associated roles. In this sense, Piquero and Benson concluded that white-collar offenders have a different "opportunity structure" than do street criminals. This reinforces the idea that the roles insiders undertake for legitimate purposes may limit the range of illegitimate opportunities open to them.

Cornish and Clarke (1987) expanded on the discussion of the offender-context dynamic by focusing on the offense. More specifically, they developed the concept of "choice-structuring" properties, which Cornish (1994) says

> *constitute the unique blend of features which distinguish one criminal activity from another in terms of its goals, targets, victims, locations, risks, payoffs, and various complementary requirements, such as motives, expertise, special knowledge resources, co-offenders, and so on* (p. 168).

Because each offense has a unique blend of choice-structuring properties, an offender must meet a series of requirements in order to successfully carry out the offense. As noted, these could include specialist knowledge, appropriate resources, and so on. In the organizational context, this could explain the relatively limited nature of insider opportunities and hence why, as Piquero and Benson (2004) noted, the opportunities open to them are "structured" by their legitimate roles. For example, an employee in the marketing department of an organization may have access to customer data, which could be sold to a competitor. Thus, the employee's position and skills help to structure the criminal opportunities open to him or her. Employees in the finance department are unlikely to be able to exploit the very same opportunity, given their position and skills. However, their job may afford opportunities for embezzlement, because they have the abilities and access to exploit the online bookkeeping system, which they use in their everyday work.

The above discussion leads to our third research question:

**Future Research Question 3:** How are potential opportunities for ICA shaped by the roles and associated skills of insiders?

As noted, scant attention has been paid to the issue of foresight and planning in the ISec literature, but the RCT framework affords a consideration of this element of ICA. Interestingly, given the relatively unique position of insiders, it may well be that they become aware of potential opportunities prior to the development of a specific motivation. As Benson and Moore (1992, p. 269) noted,

> *The bank employee's ever-present opportunity to embezzle may be resisted, for example, when all is going well. But in the case of a family member's expensive illness or a reversal of financial fortunes, the same employee may feel compelled to embezzle.*

This further illustrates the complexity of the offender decision-making process, particularly in the organizational context. Although mapping out the elements of this process for ICA presents a challenge, we argue that it is better to have a clear view of offender decision-making than a myopic view erroneously focused solely on intention.

## 4.4 Determining Which Outcomes to Measure and Obtaining Black-hat Data

Turning from the three general areas for future research we have proposed, we cannot overemphasize that in proposing the application of a full RCT perspective to DT, we are not advocating the creation of large combined models that predict intentions, as has been done for compliance intentions (Bulgurcu et al., 2010) and noncompliance intentions (Hu et al., 2011). These early efforts enriched the ISec literature, but we do not advocate the use of their approach in future research. Instead, we insist that it is time to move on to something bolder. That is, a full RCT perspective allows for the correct causal ordering of factors, which can replace the assumption that all factors influence intention. Going forward, ISec researchers should examine a causal chain of factors, such as readiness, initial involvement, intentions, behaviors, and different deterrence stages (e.g., absolute versus restrictive deterrence).

Clearly, this is a tall order that will likely require better application of existing methods. This is where scenarios-based studies may come up particularly wanting. Although scenarios can be useful for reducing social desirability bias, they are not particularly good for understanding a chain of events that unfolds in the real world. The use of intentions to study deterrence in response to hypothetical scenarios is common not only in ICA studies but also in the general criminological research on deterrence; however, a recent study by Loughran, Paternoster, & Thomas (2014) suggested that a great deal of caution should be exercised when drawing conclusions from

deterrence-type studies that rely on hypothetical scenarios and intentions to offend. This alone needs to be further examined in future research.

A partial solution to the one-time, cross-sectional scenarios problem is for ISec researchers to move toward longitudinal self-report studies, as is being done increasingly in criminological research. This approach allows researchers to observe the natural unfolding of a causal chain of events that can be reasonably deduced, including the introduction of controls and treatments. Unfortunately, the key problem with this approach is that it could reintroduce the one key problem that scenarios resolve: social desirability bias. Clearly, the more nefarious the behavior, the less likely it is to be confessed, even under the veil of anonymity.

One way this can be addressed in workplace studies is through matched studies, similar to that recently conducted in a ISec compliance context on extra-role behaviors by Hsu, Shih, Hung, & Lowry (2015). In their study, the employees' managers and supervisors (as matched to the respondents) reported on the employees' in-role and extra-role security behaviors. In a similar manner, ISec researchers could have employees complete self-report responses regarding their perceptions and demographic factors that relate to DT and RCT—and then have managers report on their employees' known ICA behaviors. Of course, such responses would likely underreport ICA, because managers do not necessarily know about ICA until the perpetrator confesses or is caught; thus, any significant findings would likely have much larger effects in reality.

Monitoring employee behavior is already an unwieldy task for managers, and ICA can be especially vexing to ferret out and resolve. Thus, an additional approach could be to employ threat awareness initiatives that have been traditionally used to monitor and thwart external attacks, and to leverage these internally (Cole, 2014; Costa, Albrethsen, Collins, Perl, Silowash, & Spooner, 2016; NIST, 2014). Increasingly, such initiatives rely on big-data monitoring and analysis techniques to look for unusual behavioral patterns in order to identify fraudulent activities, maleficence, unauthorized entry, and so on. More ISec researchers thus need to consider big-data analytics as an approach to detecting actual, real-time ICA behaviors (cf. Cardenas, Manadhata, & Rajan, 2013; cf. Edwards & Keiser, 2015) and should perhaps supplement these with self-reports.

The use of deception to identify employees willing to engage in actual ICA may be highly useful for avoiding organizational harm and would yield excellent data. However, this practice raises serious ethical issues. This has long been a common, even advocated, practice for thwarting external attacks (e.g., use of honeypots and watermarks) (e.g., Heckman, Stech, Schmoker, & Thomas, 2015). Similar approaches could be used, for example, to allow looser access to classified (but fake) documents that are watermarked to attract employees prone to leaking classified information, engaging in insider trading, and committing fraud. Watermarking allows organizations to know who leaked the documents. The honeypot concept could also be used to lure employees to access harmless, fictional data that is tracked. Although this sounds like the stuff of spy movies, hospitals have begun to use such approaches—for instance, placing watermarks in sensitive medical images—to avoid HIPPA violations due to privacy breaches (Li, Narayanan, & Poovendran, 2004).

In phishing research, deception is used to great effect to lure phishing victims in an ecologically valid manner, such that they are literally phished by the researchers using the same techniques as unauthorized phishers, but under agreement with the target organization (e.g., Wright, Jensen, Thatcher, Dinger, & Marett, 2014). In such studies, ethical review boards will typically require that researchers debrief or even train those who fall prey to phishing studies. This is a net positive, because these phishing "victims" learn how to avoid falling prey to real phishing. Similar approaches could be used in setting up honeypots and watermarks to determine who is likely to commit ICA in an organization. The great advantage of deception for research purposes is that it can be used to truly identify ICA behaviors and the individuals prone to it in a controlled and ecologically valid environment, which, in contrast to phishing studies, it is accompanied by little risk of harm for the organization. The key issue here, however, is how to deal with employees who become involved in such behaviors. Legal and ethical review board considerations will likely require such research to stop the employees before they commit actual illegal acts (e.g., after they attempt to gain unauthorized access but before they actually gain it) and then to debrief and train them without reprisal. The ISec researchers who first do this will certainly discover a methodological gold mine.

Finally, several of these issues could be resolved by examining them at the organizational level and with secondary data. For example, publicly traded organizations could be selected and classified according to known aggregated factors associated with DT and RCT constructs, using secondary data and surveys of organizational members. This information could then be linked to data from secondary news reports (e.g., Lexus/Nexus) of actual ICA reported in the news or ICA that is required to be disclosed per the Sarbanes-Oxley Act, HIPPA regulations, and so on. These kinds of secondary data studies are already used to great effect to investigate fraud and compliance issues in accounting; certainly,

they could be similarly leveraged in an organizational security context, as has been recently done by Baskerville, Hee Park, & Kim (2014). Such studies simply need to be better positioned to gather DT and RCT constructs from either surrogate secondary data or key organizational stakeholders.

# 5 Contributions

This study makes two significant contributions to the study of deterrence. First, we demonstrate how DT can be applied within a rational choice framework (e.g., Clarke & Cornish, 1985). Although previous research has suggested that DT should be incorporated within RCT (D'Arcy & Herath, 2011), no study has explained how to achieve this and the implications of doing so. Notably, neither deterrence theorists in the field of criminology nor those in the field of ISec have clearly specified the particular decisions that are influenced by the assessment of sanctions (Paternoster, 1989b; Piliavin et al., 1986). Indeed, the existing ISec deterrence studies have generally assumed that the only decision made by the offender is with regard to the *intention* to perform a certain behavior. This assumption makes it impossible to incorporate DT within an RCT framework, because RCT explicitly recognizes that the offender makes a number of choices related to a series of stages in the criminal decision-making process. Furthermore, the choices within each stage are affected by different causal factors.

RCT's acknowledgement of the complexity of the criminal decision-making process affords the application of two forms of deterrence, *absolute* and *restrictive* (Clarke & Cornish, 1985; Gibbs, 1975; Paternoster, 1989a). We demonstrate how absolute and restrictive deterrence can be aligned with what are termed the *initial involvement* and *event* stages of the RCT framework. The initial involvement stage encompasses an employee's decisions regarding whether criminal or legitimate means will satisfy their needs. If a potential offender decides that criminal behavior will address their needs, they will have decided to participate in crime and reached a state of *readiness*. It is only later, during the event stage, that an offender will commit the criminal act. Thus, the RCT framework considers deterrence in the traditional manner, noting that an offender can be deterred from committing further criminal acts (i.e., *restrictive deterrence*), which impacts the frequency of offending. However, it also affords a specific consideration that an individual may be deterred from ever participating in crime (i.e., *absolute deterrence*). This conceptual distinction provides much needed clarity in terms of understanding whom can be deterred and when.

Our second contribution is that advancing the RCT framework can open up new research areas that were previously obscured by oversimplified conceptualizations of offender decision-making. Indeed, in Section 4 of our paper, we outline three areas for future study, each with a related and overarching research question. Thus, that section opens with a reiteration of the need to examine DT from an RCT perspective. This is followed by a discussion of the first area for future research, which is accompanied by a specific call to use RCT as a basis for researching absolute and restrictive deterrence. In addition, and as just noted, it is during the initial involvement stage that a potential offender will consider whether legitimate or criminal behavior will satisfy their needs. Such a decision will be influenced by the motivations that underpin these needs. In the current ICA deterrence literature, "motivations" have been considered solely with regard to the criminal act, but this overlooks *why* an individual would initially consider participating in ICA. This "why" can, therefore, be considered through an examination of these ICA motivations at the initial involvement stage.

In addition, considering the roles undertaken by employees can illuminate how their skills and abilities can delimit or structure the ICA opportunities open to them. Thus, what might constitute an opportunity for an organization's accountant, via the online bookkeeping system, would be unlikely to represent a similar opportunity for a marketing employee in the same organization. The staff member of the marketing department would neither have access to the online bookkeeping system nor the skills and knowledge to process, for example, a fraudulent invoice.

# 6 Conclusion

Although ICA represents a significant threat for organizations, and despite numerous calls to examine this form of behavior, the academic response thus far has been scant. However, the issue of deterrence has drawn the attention of security researchers through an examination of its influence in an organizational context. Although some studies have applied DT to ICA, the manner in which this has been done has resulted in many missed opportunities: these studies have focused mainly on noncriminal security policy violations instead of ICA; they have used hypothetical scenarios instead of real behaviors; they have used cross-sectional studies instead of longitudinal and experimental designs; they have overlooked the natural extension of RCT to improve DT; they have lacked a complete understanding of absolute versus restrictive deterrence; and they have generally ignored the decision-making process and opportunities that motivate the decision to commit ICA.

Given these exciting opportunities, the purpose of this research-perspective article is to advance a deterrence research agenda based on the leading criminological

deterrence literature. Drawing on the distinction between absolute and restrictive deterrence and aligning these forms of deterrence within a rational choice framework enables the use of deterrence to influence the participation in and frequency of ICA. Therefore, our paper proposes three areas for future research on the deterrent effects of ICA, each of which is anchored in a more general RCT rather than merely in an examination of deterrence as an isolated construct.

## References


Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology, 30*(1), 47–88.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, 39,* 145–159.

Baskerville, R., Hee Park, E., & Kim, J. (2014). An emote opportunity model of computer abuse. *Information Technology & People, 27*(2), 155–181.

Benson, M. L., & Kerley, K. R. (2000). Life course theory and white-collar crime. In H. Pontell & D. Shichor (Eds.), *Contemporary issues in crime and criminal justice: Essays in honor of Gilbert Geis* (pp. 121–136). Upper Saddle River, NJ: Prentice Hall.

Benson, M. L., & Moore, E. (1992). Are white-collar and common offenders the same? An empirical and theoretical critique of a recently proposed general theory of crime. *Journal of Research in Crime and Delinquency, 29*(3), 251–272.

Blumstein, A., Cohen, J., & Farrington, D. P. (1988). Criminal career research: Its value for criminology. *Criminology, 26*(1), 1–35.

Blumstein, A., Cohen, J., Roth, J., & Visher, C. (1986). *Criminal careers and "career criminals"* (Vol. 2). Washington, DC: National Research Council.

Borenstein, M., Hedges, L. V., Higgins, J. P., & Rothstein, H. R. (2011). Introduction to meta-analysis. West Sussex, U.K.: Wiley

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *MIS Quarterly, 39*(4), 837–864.

Brantingham, P., & Brantingham, P. (1991). *Environmental criminology* (2nd ed.). Prospect Heights, IL: Waveland.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Cappelli, D., Keeney, M., Kowalski, E., Moore, A., & Randazzo, M. (2004). Insider threat study: Illicit cyber activity in the banking and finance sector. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50287

Cappelli, D. M., Moore, A., & Trzeciak, R. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud).* Boston, MA: Addison-Wesley Professional.

Cardenas, A. A., Manadhata, P. K., & Rajan, S. P. (2013). Big data analytics for security. *IEEE Security & Privacy, 11*(6), 74–76.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2013). Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157–188.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*(B), 447–459.

Choi, M. S., Levy, Y., & Hovav, A. (2013, December). *The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse.* Paper presented at the Workshop on Information Security and Privacy, Milan, Italy,

Chuma, R. J. (2012). *Investigating the impact of self-control and deterrents on noncompliant information security behavior* (Unpublished doctoral dissertation). Nova Southeastern University, Fort Laudedale, FL.

Clarke, R., & Cornish, D. (1985). Modelling offender's decisions: A framework for policy and research. In M. Tonry & N. Morris (Eds.), *Crime and justice: An annual review of research* (Vol. 6, pp. 147–185). Chicago, IL: University of Chicago Press.

Cloward, R. A., & Ohlin, L. E. (2013). *Delinquency and opportunity: A study of delinquent gangs* (Vol. 6). New York, NY: Routledge.

Cole, E. (2014). Insider threats in law enforcement. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-law-enforcement-35402

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. Clarke (Ed.), *Crime prevention studies* (Vol. 3, pp. 151–196). Monsey, NJ: Criminal Justice Press.

Cornish, D., & Clarke, R. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933–947.

Cornish, D. B., & Clarke, R. V. (2014). *The reasoning criminal: Rational choice perspectives on offending*. New Brunswick, NJ: Transaction.

Costa, D. L., Albrethsen, M. J., Collins, M. L., Perl, S. J., Silowash, G. J., & Spooner, D. L. (2016). An insider threat indicator ontology. Retrieved from http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_454627.pdf

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101.

Currie, W. (2009). Contextualising the IT artifact: Towards a wider research agenda for IS using institutional theory. *Information Technology & People, 22*(1), 63–77.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091–1124.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643–658.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113–117.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59–71.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security, 7*(4), 171–175.

Dugo, T. M. (2007). *The insider threat to organizational information security: A structural model and empirical test* (Unpublished doctoral dissertaion). Auburn University, Auburn, AL.

Edwards, J., & Keiser, E. (2015). How DoD is making cyberattacks more costly, less successful. C4ISRNET. Retrieved from http://www. c4isrnet.com/story/military-tech/cyber/2015/08/05/raising-cost-cyberattacks/31173505/

Ernst & Young. (2014). Get ahead of cybercrime: Ernst and Youngs's global information security survey 2014. Retrieved from http://www.ey. com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

Fan, J., & Zhang, P. (2011, June). *Study on e-government information misuse based on general deterrence theory.* Paper presented at the 8th International Conference on Service Systems and Service Management, Tianjin, China.

Farrinton, D. (2003). Developmental and life-course criminology: Key theoretical and empirical issues: The 2002 Sutherland award address. *Criminology, 41*(2), 221–256.

Gibbs, J. P. (1975). Crime, Punishment, and Deterrence. New York, NY: Elsevier.

Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems, 13*(4), 29–47.

Grasmick, H. G., Bursik, R. J., & Kinsey, K. A. (1991). Shame and embarrassment as deterrents to noncompliance with the law the case of an antilittering campaign. *Environment and Behavior, 23*(2), 233–251.

Grasmick, H. G., & Green, D. E. (1980). Legal punishment, social disapproval and internalization as inhibitors of illegal behavior. *Journal of Criminal Law and Criminology, 71*(3), 325–335.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: a mediating model. *Information & Management, 49*(6), 320–326.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236.

Hagan, J. (1997). Defiance and despair: Subcultural and structural linkages between delinquency and despair in the life course. *Social Forces, 76*(1), 119–134.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257–278.

Heckman, K., Stech, F., Schmoker, B., & Thomas, R. (2015). *Denial and deception in cyber defense. Computer, 48*(4), 36–44.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 28*(2), 106–125.

Higgins, G. E., Wilson, A. L., & Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture, 12*(3), 166–184.

Hirschi, T. (2002). *Causes of delinquency*. New Brunswick, NJ: Transaction.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal, 4*(1), 2–12.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49*(2), 99–110.

Hsu, J., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). How extra-role behaviors can improve information security policy effectiveness. *Information Systems Research*, *26*(2), 282–300

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54–60.

James, T., Nottingham, Q., & Kim, B. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information Technology and Management, 14*(2), 69–89.

Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139–154.

Lee, A. S., Thomas, M., & Baskerville, R. L. (2015). Going back to basics in design science: From the information technology artifact to the information systems artifact. *Information Systems Journal, 25*(1), 5–21.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management and Computer Security, 10*(2), 57–63.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707–718.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635–645.

Li, M., Narayanan, S., & Poovendran, R. (2004, September). *Tracing medical images using multi-band watermarks.* Paper presented at the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, San Francisco, CA.

Liao, Q., Luo, X., Gurung, A., & Li, L. (2009). Workplace management and employee misuse: Does punishment matter? *Journal of Computer Information Systems, 50*(2), 49–59.

Loughran, T. A., Paternoster, R., & Thomas, K. (2014). Incentivizing responses to self-report questions in perceptual deterrence studies: An investigation of the validity of deterrence theory using bayesian truth serum. *Journal of Quantitative Criminology, 30*(4), 677–707.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546–563.

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193–230.

Lowry, P. B., Posey, C., Roberts, T. L., & Bennett, R. J. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. Journal of Business Ethics, 121(3), 385–401.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: an editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431–433.

Matsueda, R. L., Kreager, D. A., & Huizinga, D. (2006). Deterring delinquents: A rational choice model of theft and violence. *American Sociological Review, 71*(1), 95–122.

Nagin, D. (1998). Criminal deterrence research at the outset of the twenty-first century. In M. Tonry (Ed.), *Crime and justice: A review of research* (Vol. 23, pp. 1–42). Chicago, IL: The University of Chicago Press.

Nagin, D. S., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law & Society Review, 27*(3), 467–496.

NIST. (2014). Framework for improving critical infrastructure cybersecurity (version 1.0). Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Pahnila, S., Siponen, M., & Mahmood, A. (2007a, January). *Employees' behavior towards IS security policy compliance*. Paper presented at the 40th Annual Hawaii International Conference on System Sciences, Waikoloa, HI.

Pahnila, S., Siponen, M., & Mahmood, A. (2007b, July). *Which factors explain employees' adherence to information security policies? An empirical study*. Paper presented at the 11th Pacific-Asia Conference on Information Systems, Auckland, New Zealand.

Paternoster, R. (1989a). Absolute and restrictive deterrence in a panel of youth: Explaining the onset, persistance/desistance, and frequency of delinquent offending. *Social Problems, 36*(3), 289–309.

Paternoster, R. (1989b). Decisions to participate in and desist from four types of common delinquency: Deterrence and the rational choice perspective. *Law & Society Review, 23*(1), 7–40.

Paternoster, R. (2010). How much do we really know about criminal deterrence. *Journal of Criminal Law & Criminology, 100*(3), 765–824.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review, 30*(3), 549–584.

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. Journal of *Management Information Systems, 20*(1), 153–177.

Piliavin, I., Gartner, R., Thornton, C., & Matsueda, R. (1986). Crime, deterrence, and rational choice. *American Sociological Review, 51*(1), 101–119.

Piquero, A. (2008). Taking stock of developmental trajectories of criminal activity over the life course, In A. Liberman (Ed.), The Long View of Crime: A Synthesis of Longitudinal Research (pp. 23–78). Washington DC: Springer.

Piquero, A., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly, 13*(3), 481–510.

Piquero, N., & Benson, M. (2004). White-collar crime and criminal careers: Specifying a trajectory of punctuated situational offending. Journal of Contemporary *Criminal Justice, 20*(2), 148–165.

Posey, C., Bennett, R. J., Roberts, T. L., & Lowry, P. B. (2011). When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security, 7*(1), 24–47.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189–1210.

PwC. (2015). Managing cyber risks in an interconnected world: Key findings from the global state of information security survey. Retrieved from http://www.pwccn.com/home/eng/rcs_info_security_2015.html

Rosenthal, R. (1979). The file drawer problem and tolerance for null results. *Psychological Bulletin, 86*(3), 638–641.

Sampson, R., & Laub, J. (2005). A life-course view of the development of crime. *The Annals of the American Academy of Political and Social Science, 602*(1), 12–45.

Sampson, R. J., & Laub, J. H. (1995). *Crime in the making: Pathways and turning points through life.* Cambridge, MA: Harvard University Press.

Schuessler, J. H. (2009). *General deterrence theory: Assessing information systems security effectiveness in large versus small businesses* (Unpublished doctoral dissertation). University of North Texas, Denton, TX.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In *New approaches for security, privacy and trust in complex environments* (pp. 133–144). New York, NY: Springer.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64–71.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296–302.

Straub, D. W. (1990). Effective IS security. *Information Systems Research, 1*(3), 255–276.

Straub, D. W., Jr. (1986). *Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment* (Unpublished doctoral dissertation). Indiana University, Graduate School of Business, Bloomington, IN.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472–484.

Ugrin, J. C., Pearson, J. M., & Odom, M. D. (2008). Cyber-slacking: Self-control, prior behavior and the impact of deterrence measures. *Review of Business Information Systems, 12*(1), 75–87.

Ugrin, J. C., & Pearson, M. J. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior, 29*(3), 812–820.

Wall, J. D., Lowry, P. B., & Barlow, J. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems, 17*(1), 39–76.

Warkentin, M., Malimage, N., & Malimage, K. (2012, December). Impact *of protection motivation and deterrence on is security policy compliance: a multi-cultural vi*ew. Paper presented at the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC), Orlando, FL.

Warkentin, M., McBride, M., Carter, L., & Johnston, A. (2012, August). *The role of individual characteristics on insider abuse intentions.* Paper presented at the Americas Conference on Information Systems, Seattle, WA

Weisburd, D. (1991). *Crimes of the middle classes: White collar offenders in the federal courts*. New Haven, CT: Yale University Press.

Weisburd, D., & Waring, E. (2001). White-collar crime and criminal careers. New York, NY: Cambridge University Press.

Wheeler, S., Weisburd, D., Waring, E., & Bode, N. (1988). White collar crime and criminals. *American Criminal Law Review, 25*(3), 331–357.

Whetten, D., Felin, T., & King, B. (2009). The practice of theory borrowing in organizational studies: Current issues and future directions. *Journal of Management, 35*(3), 537–563.

Willison, R. (2006). Understanding the offender/environment dynamic for computer crime. Information *Technology & People, 19*(2), 170–186.

Willison, R. & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1–20.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, 28(2), 266–293.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology, 58*(2), 212–222.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research, 25*(2), 385–400.

Wu, J., & Lederer, A. (2009). A meta-analysis of the role of environmentbased voluntariness in information technology acceptance. *MIS Quarterly, 33*(2), 419–432.

Wu, J., & Lu, X. (2013). Effects of extrinsic and intrinsic motivators on using utilitarian, hedonic, and dual-purposed information

systems: A meta-analysis. *Journal of the Association for Information Systems, 14*(3), 153–191.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management, 24*(4), 281–287.

Zhang, L., Smith, W. W., & McDowell, W. C. (2009). Examining digital piracy: SAelf-control, punishment, and self-efficacy. *Information Resources Management Journal, 22*(1), 24–44.

# Appendix A. Literature Review of DT in the Workplace

We conducted a systematic literature review to complete the Table A1 in this appendix and to further establish several of the points in our manuscript. Our primary objective was to find publications that dealt with a combination of deterrence theory and employee security behaviors in the workplace. This was not a meta-analysis, but instead, a comprehensive review. But like meta-analyses, comprehensive reviews are biased when they intentionally omit lower-quality publications, because it turns out that top peer-reviewed journals expect significant results, so results that are mixed or insignificant are less likely to be published in top journals. This phenomenon distorts scientific results, and is a serious widely known problem called the "file drawer" problem (Borenstein, Hedges, Higgins, & Rothstein, 2011; Rosenthal, 1979). That is, if a study does not turn out as expected, it virtually never gets past the conference or dissertation stage, or ends up in a lower-quality journal (Rosenthal, 1979). Thus, proponents of systematic review and meta-analysis insist that the literature included be inclusive and not be filtered for perceived "lower-quality" publications (Borenstein et al., 2011; Rosenthal, 1979; Wu & Lederer, 2009; Wu & Lu, 2013). For this reason, we cannot have a balanced understanding of the DT security literature, without considering the whole of the literature; otherwise, it is ironically more positively skewed to more likely positive results in top journals. Accordingly, we included dissertations, conferences, and journal articles. Likewise, this is also why we placed no restrictions on which field or which journals were used. We wanted all DT-related security papers, not just ones published in IS journals or conferences. We likewise placed no restrictions on the date ranges of the articles.

To find a reasonable population of such articles, we followed an approach of search oversampling, which is commonly done with meta-analytic studies. Essentially the idea here is to have two or more researchers searching for articles independently (in our case, it was the authors and two PhD students), and combining them into the same repository until no new articles could be found. We did so, using the following partially redundant article information repositories:

- Search EBSCO Business Source Complete.
- Search ABI/INFORM Business
- Search Web of Science
- Search Google Scholar
- Search the AIS library

When a new article was found that was in our review scope, its bibliography was checked for potentially overlooked articles. The article was then entered into Google Scholar to examine all its citing articles, to find other potential overlooked articles.

In terms of the search terms, we were careful to make sure that the *full-text* of an article had either "deterrence" or "deterrence theory" or "general deterrence theory" in it, AND had the word "security" AND had at least one of the following terms: (Compliance, Computer abuse, Computer crime, Fear appeals, Information misuse, Information security policies/policy, Malicious, Noncompliance, Policy compliance, Protection motivation, Rational choice, Security awareness, Security concern, Security countermeasures, Security policy, Threat, Violation). We earlier learned that such searches on keywords and abstracts were unreliable, as usually one of the key parts was often missing and thus key articles were overlooked.

Through this process there were a good number of articles that appeared to be promising but were out of scope. This usually occurred because the article was a conceptual article or it was an article that used DT for the context of encouraging policy *compliance.* For example, Dhillon (1999) is an early conceptual piece on deterrence of security violations; Lee and Lee (2002) was not included, as it is a theoretical essay; Kankanhalli et al. (2003) was not included because it is an organization-level study; Theoharidou, Kokolakis, Karyda, & Kiountouzis (2005) is a conceptual piece on deterrence; Higgins et al. (2005) used DT in an empirical study of deterring study software piracy; Guo et al. (2011) addresses nonmalicious security violations; Willison and Warkentin (2013) was a conceptual piece about deterrence and more.

Once we found all of the articles that were in scope, we carefully read them and coded them. We especially wanted to document the degree to which they dealt with criminal computer abuse, as some dealt with a mix of illegal activities and nonillegal activities. We also examined whether the study was one involving organizational employees and DT, and the specifics of the method. Table A1 summarizes our efforts.

**Table A1. Summary of the Major Literature that has Used DT in a Security Compliance/Noncompliance Context**

| Citation (Study type) | Criminal / malicious context? | Participants | DV type | Other theories / constructs | Method | Findings / application to DT |
|---|---|---|---|---|---|---|
| Barlow et al. (2013) (ISI) | No (IT policy violation intention) | Employees | Scenarios (negative) | Neutralization theory | Factorial survey | Focused on "communication of deterrent sanctions" as one overall DT-related construct. Showed this construct and some neutralization constructs lowered intentions to violate IT policies. |
| Bulgurcu et al. (2010) (ISI) | No (ISP compliance intention) | Employees | Intentions (positive) | RCT and TPB | Cross-sectional survey | Study was not a true DT study, but is often miscited as such. It was primarily based on RCT and TPB. However, they showed that sanctions had a positive relationship with cost of noncompliance, which predicted compliance attitude, and then intentions. |
| Chen et al. (2013) (ISI) | No (ISP compliance intention) | Employees | Scenarios (positive) | Reward, security training, monitoring, training, policy | Factorial survey | In addition to severity and certainty, they added reward. All were shown to positively influence compliance intentions. |
| Cheng et al. (2013) (ISI) | No (ISP violation intention) | Employees | Scenarios (negative) | Social control (social bonds and pressure) | Factorial survey | Added several subconstructs of social bonds and social pressure to certainty and severity. Certainty was insignificant; severity was significant. Several of the social control constructs were significant. |
| Chuma (2012) (thesis) | No (noncompliant, nonmalicious security behavior) | Employees at one company | Behaviors (negative) | Self-control theory, social bonding | Cross-sectional survey | Used certainty, severity, and celerity. Severity was insignificant whereas certainty and celerity were significant. Dealt with nonmalicious noncompliance behaviors such as write down password, share password, not verifying sending of email, opening email attachments without knowing. |
| D'Arcy & Devaraj (2012) (ISI) | Partial (IS misuse intentions; not strong criminal intent) | Employees, including part-time MBA students | Scenarios (negative) | Informal sanctions as DT extension | Factorial survey | Examined formal sanctions (combined severity/certainty) and added informal sanctions (social desirability and moral beliefs). All three were significant. All participants were given four scenarios and all measures were averaged from the four scenarios and analyzed together. |
| D'Arcy & Hovav (2007) (ISI) | Partial (IS misuse intentions; not strong criminal intent) | Employees, including part-time MBA students | Intentions (negative) | n/a | Factorial survey | Did not directly use DT constructs, but argued that ISPs, SETA programs, monitoring, and preventive security software are deterrence surrogates that reduce IS misuse intentions. All were significant except computer monitoring. |

**Table A1. Summary of the Major Literature that has Used DT in a Security Compliance/Noncompliance Context**

| | | | | | | |
|---|---|---|---|---|---|---|
| D'Arcy & Hovav (2009) (ISI) | Partial (unauthorized access/modification intent) | Employees, including part-time MBA students | Intentions (negative) | Moral judgment | Cross-sectional survey | Did not directly use DT constructs, but argued "security countermeasures" of ISPs, acceptable use guidelines, monitoring and SETA programs are deterrence surrogates that reduce IS misuse intentions. Moral judgement was the strongest factor whereas mixed support was found for the deterrence surrogates |
| D'Arcy et al. (2009) (ISI) | Partial (IS misuse intentions; not strong criminal intent) | Employees | Scenarios (negative) | Moral commitment | Factorial survey | Showed that severity, but not certainty, was associated with decreased IS misuse intentions. Also, added moral commitment as a negative influencer. Other factors were also examined to predict certainty and severity. Four scenarios: (1) email joke, (2) use restricted information to ask for a raise, (3) unlicensed software, (4) round-up work hours. All participants were given four scenarios and all measures were averaged from the four scenarios and analyzed together. |
| Fan & Zhang (2011) (conference) | No (nonstandard threats behavior DV) | Employees | Nonstandard DV | n/a | Cross-sectional survey | Used security policies, SETA programs, monitoring, and preventative software as surrogates of DT's concept of deterrence. They ran all of these against four kinds of information threats as DVs, contrary to the general literature, and mixed results were obtained. |
| Guo & Yuan (2012) (ISI) | No (intentions to violate policies) | Employees | Scenarios (negative) | Personal sanctions | Factorial survey | Conceived of sanctions on organizational, workgroup, and personal levels. Organizational sanctions were insignificant, whereas personal and workgroup sanctions were significant. They did not distinguish severity/certainty of sanctions. |
| Guo et al. (2011) (ISI) | No (nonmalicious security violation intentions) | Employees | Scenarios (negative) | ISP attitude, relative advantage, risk, norms, identity match | Factorial survey | Added several unrelated constructs to sanctions (combined certainty/severity). Used this to predict attitudes toward nonmalicious security violation intentions. Sanctions was insignificant as was attitude toward ISP. Attitudes predicted intentions. |
| Harrington (1996) (ISI) | Yes (computer abuse) | IS employees | Scenarios (negative) | Ethical judgments (denial of responsibility) | Factorial survey | This is not directly a DT study. However, they used corporate codes of ethics as deterrence surrogates in their study and used DT literature to justify this decision. Scenarios involved true criminal computer abuse: cracking, sabotage, purposeful virus spread, software theft, fraud. Showed corporate codes did not reduce intent; however. they did serve to reduce denial of responsibility. |
| Herath & Rao (2009a) (ISI) | No (ISP compliance intentions) | Employees | Intentions (positive) | Social pressure/extrinsic motivation; perceived effectiveness/intrinsic motivation | Cross-sectional survey | Severity was insignificant whereas certainty was significant in increasing ISP compliance intention. Social pressure (normative beliefs and peer behavior) and perceived effectiveness were also significant. |

**Table A1. Summary of the Major Literature that has Used DT in a Security Compliance/Noncompliance Context**

| | | | | | | |
|---|---|---|---|---|---|---|
| Herath & Rao (2009b) (ISI) | No (ISP compliance intentions) | Employees | Intentions (positive) | Protection motivation theory (PMT), theory of planned behavior (TPB) | Cross-sectional survey | Model mixed DT, PMT, and TPB. Severity decreased intentions whereas certainty increased intentions. ISP attitude had no effect; whereas organizational commitment, self-efficacy, and norms were significant. |
| Hovav & D'Arcy (2012) (ISI) | Partial (IS misuse intentions; not strong criminal intent) | Employees, including part-time MBA students | Scenarios (negative) | Moral beliefs | Factorial survey | Examined DT in U.S. versus Korea context. All participants were given four scenarios and all measures were averaged from the four scenarios and analyzed together. Examined severity and certainty. Certainty was significant for U.S. sample but severity was not; severity was significant for Korean sample but certainty was not. |
| Hu et al. (2011) (ISI) | Yes (criminal computer abuse) | Employees | Scenarios (negative) | RCT, self-control, shame, moral beliefs | Factorial survey | Used certainty, severity, and celerity of sanctions. In model these three directly predicted informal and formal risks. Separate model showing these three against negative intentions showed no significance. Only extrinsic and intrinsic benefits were directly significant. Three computer abuse scenarios: unauthorized access for gain, steal/sell commercial secret, steal/sell product info. |
| Kankanhalli et al. (2003) (ISI) | No (looked at IT security effectiveness) | IT managers | Manager assessment of security effectiveness (positive) | Deterrent efforts; preventative efforts | Cross-sectional survey | Examined how deterrent efforts (representing certainty), deterrent severity, and preventive efforts lead to IS security effectiveness, and the demographics factors that influence the underlying predictors. No direct measure of anything criminal or of malicious nature. Severity was significant for U.S. participants whereas certainty was significant for Korean participants |
| Lee et al. (2004) (ISI) | Yes (computer abuse) | Employees | Intentions & behaviors (negative) | Social control | Cross-sectional survey | Did not use certainty and severity. Instead, used security policy, security awareness, and physical security system all as "general deterrence theory" surrogates. Examined intention from participants and then added reported actual abuse from insiders and outside "invaders." Model deterrence surrogates as predictors of "self-defense intention", which then was significant modeled to decrease abuse by "invaders" and abuse by insiders. Of the surrogates, only "security system" was significant. |
| Li et al. (2010) (ISI) | No (compliance intentions with Internet use policy) | Employees | Intentions (positive) | RCT | Cross-sectional survey | This was primarily an RCT-based model, but they added certainty, severity, and subjective norms (as informal sanctions). Certainty was significant whereas severity and norms were insignificant. |
| Liao et al. (2009) (ISI) | No (intentions to avoid Internet misuse) | Employees | Intentions (positive) | TPB, ethics | Cross-sectional survey | Only predicted severity and certainty to misuse attitudes (not intentions), perceived behavioral control, and subjective norms. Neither severity nor certainty significantly predicted attitudes. |

**Table A1. Summary of the Major Literature that has Used DT in a Security Compliance/Noncompliance Context**

| | | | | | | |
|---|---|---|---|---|---|---|
| Lowry et al. (2015) (ISI) | Partial (computer abuse but not all was criminal/malicious) | Employees | Behaviors (negative) | Fairness theory | Cross-sectional survey | The primary purpose of the article was testing fairness theory in the context of reactive computer abuse at work. However, the authors tested certainty, severity, and celerity as counterexplanations. They were not significant in this context. |
| Pahnila et al. (2007a) (conference) | No (ISP compliance) | Employees | Intentions (positive) | PMT, habit, norms, rewards | Cross-sectional survey | Multiple theories and constructs combined with "sanctions" from DT. Did not separate certainty/severity. Sanctions were not significant in predicting intentions, but attitudes, norms, and habits were. Intentions predicted actual compliance, but did not test sanctions against actual compliance. |
| Peace et al. (2003) (ISI) | Yes (software piracy) | Employees | Attitudes & Intentions | TPB | Cross-sectional survey | Studied employee software piracy in the workplace. Severity and certainty decreased attitude. |
| Siponen & Vance (2010) (ISI) | No (ISP violations intentions) | Employees | Scenario (negative) | Neutralization theory; shame | Factorial survey | Used extended version of DT that included informal sanctions, and added shame. Formal and informal sanctions included certainty and severity, but these were analyzed as one construct. Only neutralization was significant. |
| Siponen et al. (2007) (book) | No (ISP compliance) | Employees | Behaviors (positive) | PMT, TRA | Cross-sectional survey | Multiple theories and construct combined with "sanctions" from DT. Did not separate certainty/severity. Did not run sanctions against intentions, but instead ran them against actual compliance, and these were significant. |
| Siponen et al. (2010) (ISI) | No (ISP compliance) | Employees | Intentions & behaviors (positive) | PMT, TPB, visibility, rewards | Cross-sectional survey | Very general compliance (e.g., "I comply with information security policies"). Combined PMT and several other constructs with DT. Combined DT severity, certainty, and celerity as one construct called "deterrences," and this was a significant predictor of actual compliance.<br>Note that Pahnila et al. (2007b) was a conference version of this paper with the same data; thus, we only summarize these together here. |
| Son (2011) (ISI) | No (ISP compliance) | Employees | Behavior (positive) | Intrinsic motivation (legitimacy, value congruence), CSE | Cross-sectional survey | Both certainty and severity were insignificant whereas computer self-efficacy, legitimacy, and value congruence were significant. |
| Straub (1990) (ISI) | Yes (computer abuse) | IS management | Manager report of observed abuse (negative) | Provide basic rival explanations | Cross-sectional survey | Implementing IS security deterrents (measured as certainty and severity) decreased computer abuse.<br>Straub (1986) is the dissertation version of this article and has the same data; thus we summarize them together here. |

**Table A1. Summary of the Major Literature that has Used DT in a Security Compliance/Noncompliance Context**

| | | | | | | |
|---|---|---|---|---|---|---|
| Straub & Welke (1998) (ISI) | Yes (computer abuse) | IS management | Qualitative discussion of risk assessment | n/a | Qual. | Nonempirical qualitative study that used ideas of DT to help cope with and plan for systems risk. Not a direct test of DT, but suggested communicating sanctions as part of SETA programs. |
| Ugrin & Pearson (2013) (ISI) | No (cyberloafing) | Employees and students | Intentions (negative) | Detection, enforcement, abusiveness | Cross-sectional survey | A major measurement issue is that "sanction" was used to represent DT and they were given a cue of potential sanction of being fired or receiving a reprimand for each kind of cyberloafing. Asked about intentions for six different kinds of cyberloafing. Another major issue is that half of the respondents were students, which makes their responses to company-specific measurement items questionable. |
| Ugrin et al. (2008) (non-ISI) | No (cyberslacking) | Employees and students | Intentions (negative) | Self-control, prior behavior | Cross-sectional survey | One issue is that they equated "detection systems" to be representative of severity/certainty. Another major issue is that half of the respondents were students, which makes their responses to company-specific measurement items questionable. Analysis was also not performed in standard manner. Generally concluded detection mechanisms deter cyberslacking. Study may be more about monitoring than it is about severity/certainty: in their 2013 study Ugrin and Pearson (2013) show detection separately as a positive moderator of sanctions. |
| Warkentin, McBride, et al. (2012) (conference) | No (intentions to violate policies) | Employees | Scenarios (negative) | PMT, Big-5 personality traits | Factorial survey | Severity was significant but certainty was not; mixed results with other constructs. |
| Workman & Gathegi (2007) (ISI) | No (contravene security policies) | Employees | Behaviors (negative) | TPB, self-control, legal attitude, norms, ethical training | Field exper. | Punishment is the DT-related construct used in this study, but did not follow standard operationalizations and did not measure punishment or its manipulation. DV was about reported contravention of security measures. Punishment and ethical training negatively relate to "threat of software and information security contravention." They had control group, punishments warning group, and ethics training group. Data were collected before treatments/control and six months later. Found warning about punishments and ethics training to be helpful, depending on underlying motivations of people. |

*Note:* ISI = A highly rated, high-impact journal listed on Thomson-Reuter's ISI Web of Science; non-ISI = nonindexed journal

## About the Authors

**Robert Willison** is currently a visiting junior professor in the Faculty of Information Technology at the University of Jyväskylä. He received his PhD in Information Systems from the London School of Economics and Political Science, as well as an MSc. in Sociology from the same institution. His work has appeared in journals such as *MIS Quarterly*, *Information Systems Journal*, *European Journal of Information Systems*, *Information &Management, Information & Organization*, *Communications of the ACM*, *IT & People*, and others. He has served as an associate editor for *European Journal of Information Systems*, as well as a cotrack chair for the International Conference on Information Systems and the European Conference on Information Systems. His research covers the broad area of IS security, with the majority of his papers examining insider computer abuse.

**Paul Benjamin Lowry** is the Suzanne Parker Thornhill Chair Professor in Business Information Technology at the Pamplin College of Business at Virginia Tech. He received his PhD in management information systems from the University of Arizona and an MBA from the Marriott School of Management. He has published 110+ journal articles in *MIS Quarterly, Information Systems Research, Journal of Management Information Systems, Journal of the Association for Information Systems, Information Systems Journal, European Journal of Information Systems, Decision Sciences Journal, Information & Management, Communications of the ACM, Decision Support Systems,* and others. He is a department editor at *Decision Sciences Journal.* He also is a senior editor of *Journal of Management Information Systems, Journal of the Association for Information Systems,* and *Information Systems Journal*, and an associate editor for the *European Journal of Information Systems*. He has also served multiple times as track cochair at the International Conference on Information Systems, the European Conference on Information Systems, and the Pacific Asia Conference on Information Systems. His research interests include (1) organizational and behavioral security and privacy; (2) online deviance, online harassment, and computer ethics; (3) HCI, social media, and gamification; and (4) business analytics, decision sciences, innovation, and supply chains.

**Raymond Paternoster** (February 29, 1952–March 5, 2017) was a leading American criminologist who taught at the University of Maryland from 1982 until his death in 2017, spending much of this time as a Distinguished Professor in the Department of Criminology and Criminal Justice. Aside from being a prolific, interdisciplinary publisher of criminological research, Paternoster was widely known for his studies on racial disparities in the application of capital punishment in the United States, and research examining the application of rational choice theory. Sadly, he passed away after a valiant battle with cancer during the final writing of this manuscript. Importantly, this manuscript was inspired by his compelling, interdisciplinary work, and we dedicate this manuscript to his memory.